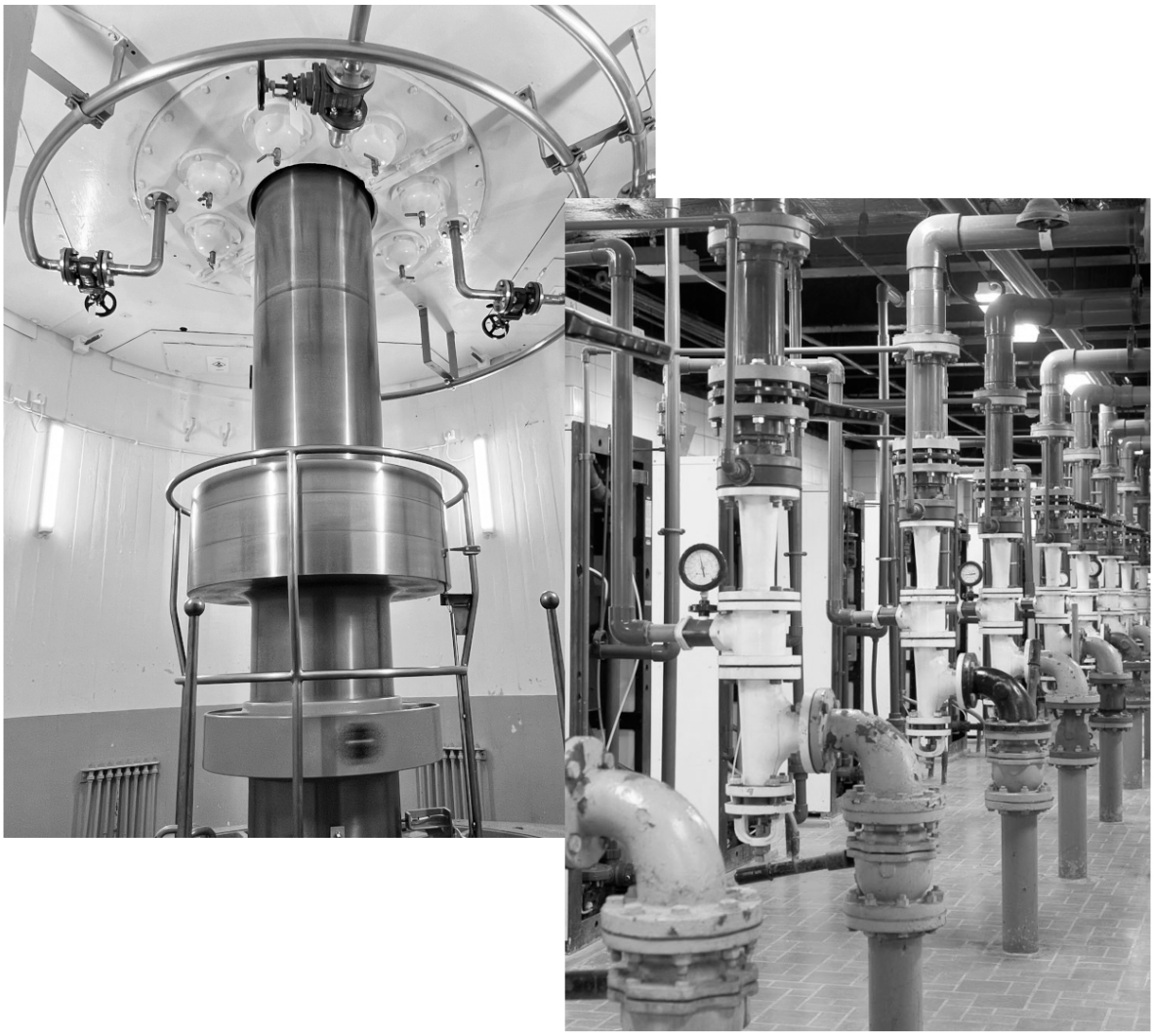
kraftCERT infraCERT



Trusselvurdering

2026

Innhold

1 Trusselvurdering 2026 . . . . . **3**
1.1 Nøkkelvurderinger 3
1.2 Usikkerhet, metode og horisont 3

2 Rammeverk for forståelse og bruk **4**
2.1 Formål og avgrensning 4
2.2 Om KraftCERT 4
2.3 Sannsynlighetsbegreper, gjeldende fra 2026 4

3 Situasjonsbildet **5**
3.1 Cyberkriminalitet 5
3.2 Statlige trusler 5
3.3 Strategisk usikkerhet og avhengigheter 6

4 Trusler mot industrielle kontrollsystemer **7**
4.1 Ubetydelige angrep / Nuisance attacks 7
4.2 Disruptive angrep og driftsforstyrrelser 8
4.3 Destruktive angrep 9

5 Kunstig intelligens (KI) i trusselbildet **10**

6 Aktører **11**
6.1 Overordnet 11
6.2 Tilretteleggere 11
6.2.1 Tjenesteleverandører 11
6.2.2 Offensive kontraktører 12
6.2.3 Innsidere 12
6.3 Cyberkriminelle 13
6.4 Oppdragsstyrte aktører 14
6.4.1 Nasjonalstater 14
6.4.2 Hacktivister 15

7 Teknikker **17**
7.1 Unified Kill Chain 17
7.2 Tilgang (In) 17
7.2.1 Kartlegging og målutvelgelse 17
7.2.2 Direkte teknisk tilgang 17
7.2.3 Angrep gjennom leverandører 19
7.3 Bevegelse (Through) 20
7.4 Iverksettelse (Out) 21

8 Om rapporten **22**
8.1 Trusselvurdering og tiltakspakke 22
8.2 Trafikklysprotokollen 22
8.3 Endringslogg 22

1 Trusselvurdering 2026

Alle virksomheter blir utsatt for trusselaktivitet. Innen IT betyr det forsøk på innpass gjennom kjente teknikker som phishing og misbruk av legitime verktøy. I OT[1] betyr det kartlegging av eksponerte tjenester, åpne porter og svakt sikret utstyr.

Kraft- og petroleumssektorene er godt regulerte sektorer med påkrevd grunnsikring i OT, men angrep i IT kan fortsatt få konsekvenser for OT gjennom funksjonelle avhengigheter. Svakt sikrede OT-systemer uten tilsvarende barrierer er mer utsatt for direkte angrep.

1.1 Nøkkelvurderinger

Kriminelle aktører er den mest sannsynlige angriperen mot virksomheter i våre sektorer.[2] Det er nesten sikkert (> 90%) at de fleste angrep vil bruke kjente inngangsveier: eksponerte tjenester, phishing og misbruk av legitime verktøy.

Det er sannsynlig (55–70%) at angrep mot IT-systemer gir driftsforstyrrende konsekvenser for kontrollsystemer der IT og OT er funksjonelt avhengige av hverandre. Isolering og nedstenging av OT som forsvarstiltak er i seg selv tilstrekkelig til å påvirke produksjonen.

Det er meget lite sannsynlig (15–20%) at vi ser vellykkede destruktive cyberangrep mot industrielle kontrollsystemer på kort sikt blant KraftCERTs medlemmer. Slike angrep krever detaljert målkunnskap, omgåelse av flere sikkerhetslag og høy ressursbruk over lang tid.

Angripere vil i økende grad bruke virksomhetens egne, legitime verktøy til å operere uoppdaget og bevege seg i nettverket. I IT-sonene er det meget sannsynlig (75–85%) at interne legitime verktøy brukes til eksfiltrasjon og effekt.

Det er meget sannsynlig (75–85%) at alle typer trusselaktører bruker KI[3] til å øke tempo og volum i angrep. KI senker produksjonstiden for skadevare og gjør skanning og phishing mer skalerbar. KI gir aktørene raskere arbeidsmetoder – ikke vesentlig nye kapabiliteter.

Det er nesten sikkert (> 90%) at russisk-støttede hacktivister vil forsøke angrep mot sårbar, internetteksponert infrastruktur i Norge. Det er lite sannsynlig (25–40%) at de oppnår driftsforstyrrende effekt mot kontrollsystemer med grunnsikring på plass. Det er høyst usannsynlig (< 10%) at russisk-støttede hacktivister oppnår destruktiv effekt, da de mangler målkunnskap og tekniske ressurser til å omgå safety-systemer.

1.2 Usikkerhet, metode og horisont

Datagrunnlaget for trusselvurderinger på feltet er svakt eller fraværende. Dette er et generelt problem for alle, både for offentlige og graderte vurderinger. Statistikker og trendbeskrivelser omkring cyberangrep er gjennomgående usikre, lite representative og det er svært mange udokumenterte påstander. KraftCERTs vurderinger er basert på kunnskap, erfaringer, observasjoner, samt kritisk lesing og analyse av eksterne rapporter, satt sammen i analytisk arbeid. Der usikkerheten er særlig stor, blir det angitt i teksten.

1 Operasjonell teknologi
2 Elkraft, Petroleum, Vann og avløp, Industriproduksjon
3 Kunstig intelligens

2 Rammeverk for forståelse og bruk

2.1 Formål og avgrensning

Trusselvurdering 2026 beskriver utviklingstrekk, trusselaktører og angrepsformer KraftCERT vurderer som mest relevante for våre sektorer. Vurderingen dekker aktørers intensjon, evne og mulighet, men omfatter ikke tekniske detaljer, individuelle trusselaktører eller helhetlige sårbarhets- og konsekvensvurderinger.

Rapporten omfatter ikke anbefalinger om spesifikke tiltak. Disse vil utarbeides og publiseres i Tiltakspakke 2026.

Rapporten ser 2–3 år frem i tid, med kort sikt vurdert til omtrent ett år. For industrielle kontrollsystemer vurderes lengre tidshorisonter. Vurderingene er ikke allmenngyldige og må leses i sammenheng med den enkelte virksomhets sårbarheter og eksponering.

2.2 Om KraftCERT

KraftCERT er operativt sektorresponsmiljø for kraft og petroleum, og ellers består målgruppen av prosess-industri, vann- og avløpssektoren samt energigjenvinning. KraftCERT har medlemmer både i Norge og på Island.

KraftCERT er både ISAC (Information Sharing and Analysis Center) og IRT (Incident Response Team) for våre medlemmer. Vi gir støtte ved digitale hendelser, og formidler relevant og verifisert informasjon om sårbarheter, trusler og angrep.

KraftCERT er del av den nasjonale beredskapen, og samarbeider med både private og offentlige aktører nasjonalt og internasjonalt.

KraftCERT er medlem av Forum of Incident Response and Security Teams (FIRST) og sertifisert IRT i Trusted Introducer.

2.3 Sannsynlighetsbegreper, gjeldende fra 2026

KraftCERT bruker faste begreper for å beskrive hvor sannsynlig det er at en hendelse eller utvikling vil inntreffe. Begrepsbruken følger Etterretningstjenestens nasjonale standard, som er endret siden vår forrige trusselvurdering i 2025.

Sannsynlighetsgrad	Prosent	Beskrivelse	NATO-standard
Nesten sikkert	> 90 %	Alt tyder på	Almost certain
Meget sannsynlig	75–85 %	Det er veldig god grunn til å forvente	Highly likely
Sannsynlig	55–70 %	Det er god grunn til å forvente	Likely
Mulig	45–50 %	Det er ikke sannsynlighetsovervekt	Possible
Lite sannsynlig	25–40 %	Det er liten grunn til å forvente	Plausible
Meget lite sannsynlig	15–20 %	Det er meget liten grunn til å forvente	Unlikely
Høyst usannsynlig	< 10 %	Ingen grunn til å forvente	Highly unlikely

3 Situasjonsbildet

«Vi må innse at verdensordenen slik vi kjente den er i oppløsning», skriver sjefen for Etterretningstjenesten i Fokus 2026[1]. Situasjonsbildet vil preges av kjente trusler i en mer uforutsigbar ramme. Opportunisme og økonomisk vinning er fremdeles de viktigste faktorene bak de fleste angrep, men også statlige trusler må tas alvorlig. Spionasje er en del av normalen. Digitale og fysiske avhengigheter blir i større grad brukt som pressmidler[1][2].

Russland er kjent. Kina er kjent. Det nye i 2026 er at vår viktigste allierte er blitt en usikkerhetsfaktor.

3.1 Cyberkriminalitet

Cyberkriminalitet er den mest vedvarende og sannsynlige trusselen. Kriminelle aktører er opportunistiske og økonomisk motiverte[3]. Flere enkle angrep mot mange mål gir ofte større samlet avkastning enn få kompliserte operasjoner. Kommersialisering, arbeidsdeling og gjenbruk av verktøy gjør terskelen lav og gjør det mulig å øke antall angrep med begrenset innsats[3]. Stjålne data og gyldige tilgangsopplysninger er sentrale varer i en kriminell økonomi der spesialiserte aktører selger videre innledende tilgang til kompromitterte systemer[4]. Slik tilgang kan deretter brukes i utpressing, bedrageri og andre angrep[4].

3.2 Statlige trusler

Russland og Kina er de mest relevante statlige trusselaktørene for KraftCERTs medlemmer. EOS-tjenestene[4] beskriver i sine åpne vurderinger at begge stater har intensjon og kapabilitet til å gjennomføre operasjoner mot vestlige mål, inkludert Norge[1][5]. Iran og Nord-Korea vurderes som mindre relevante for våre sektorer. Russland og Kina omtales nærmere i kapittel 6 om Nasjonalstater(s. 14).

Det er meget sannsynlig (75–85%) at Ukraina-krigen er den viktigste driveren for russisk interesse for Norge, som del av den vestlige blokken og som kraft- og petroleumsleverandør til Europa. Nordområdene og alliansepolitikken er de viktigste langsiktige faktorene. Virksomheter med tilknytning til Ukraina-støtte vil ha et høyere trusselnivå enn andre[1].

Spionasje er en del av normaltilstanden. Statlige aktører innhenter informasjon og etablerer tilgang i fredstid for å være forberedt på ulike utviklinger[1]. Kritisk infrastruktur, digitale avhengigheter og sårbarheter i norsk digital infrastruktur er etterspurte mål for etterretning[5]. Tilsynelatende uskyldig eller fragmentert informasjon kan over tid gi innsikt i systemer og sammenhenger som gjør det mulig å planlegge og gjennomføre angrep. Det er helheten som avgjør verdien, ikke hvert enkelt datapunkt.

Etterretningstjenesten peker særskilt på kartlegging av infrastruktur langs kysten og på havbunnen, og trekker frem fiberkabler og gassrørledninger som konkrete mål[1]. Russland har dedikerte avdelinger for slike operasjoner, og Etterretningstjenesten omtaler dem åpent for første gang i år. Slik kartlegging kan også understøtte sabotasje[1].

Sabotasje er en relevant og i hovedsak fysisk trussel mot KraftCERTs medlemmer. De mest sannsynlige målene er eiendom og logistikkinfrastruktur knyttet til støtte til Ukraina. PST bruker i 2026 sivil infrastruktur som samlebetegnelse der de tidligere brukte kritisk infrastruktur, uten en tydelig avgrensning av hva begrepet omfatter.[5].

[4] Etterretningstjenesten(E-Tj), Politiets sikkerhetstjeneste (PST), Nasjonal Sikkerhetsmyndighet (NSM)

3.3 Strategisk usikkerhet og avhengigheter

USAs stabiliserende rolle er redusert, og det påvirker trusselbildet på flere nivåer.

Kostnaden for å bryte internasjonale normer er synkende. Etterretningstjenesten beskriver et globalt skifte mot interesse- og maktpolitikk der internasjonalt samarbeid svekkes[1]. USAs endring i relasjon til Europa er både et symptom på og en driver av dette skiftet, og reduserer risikoen for Russland og andre aktører som vurderer handlinger mot europeisk infrastruktur. For våre sektorer betyr det at vurderinger som tidligere hvilte på at oppdagelse eller diplomatisk respons ville avskrekke, må revurderes. Tersklene er under press.

Det er mulig (45–50%) at avhengigheten til amerikanske skytjenester vil brukes som politisk pressmiddel, eksempelvis i en krise i forholdet mellom USA og Europa. Norge har høy markedskonsentrasjon av slike tjenester[6]. USA brukte i 2025 sanksjoner mot en embetsmann i ICC[5] som førte til at han ble frakoblet Microsofts tjenester[7]. Nyere amerikansk strategisk policy beskriver samtidig sikring av amerikanske teknologier, datasentre og leverandørkjeder som en strategisk ressurs, samt bruk av privat offensiv cyberkapabilitet[8].

Trusselpersepsjonen formes av feil eksempler

Primitive angrep og udokumenterte trusler får stor propagandaeffekt når myndigheter og media forsterker dem.

Angrepet på en dam tilknyttet fiskeoppdrett i Bremanger i april 2025 illustrerer dette. Angrepet var lite sofistikert, og anlegget er ikke på noen måte kritisk infrastruktur, men PSTs omtale på Arendalsuka og NSMs nasjonale varsel ga den prorussiske gruppen bak angrepet langt større oppmerksomhet enn de kunne oppnådd på egen hånd.

I februar 2026 fikk påstander om «trusler mot nordisk energisektor» massive nyhetsoppslag. Det var ingen konkret trussel. Svenske myndigheter og media kommuniserte uklart, og norske redaksjoner spredte saken umiddelbart.

Et gjennomgående mønster er at målvalg forklares i etterkant. Når et angrep har skjedd, konstrueres det en rasjonell intensjon om å ramme akkurat det målet, eller en sektor, eller en annen overbygning. Realiteten er oftest at angriperen utnyttet en tilgjengelig sårbarhet, og at målet ble valgt fordi det lot seg angripe, ikke fordi det var viktig.

Verken et angrep på en dam eller udokumenterte påstander på sosiale medier er gode indikatorer på hvor sårbar kritisk infrastruktur er, eller hvor alvorlig trusselbildet er.

[5] International Criminal Court

4 Trusler mot industrielle kontrollsystemer

OT er kjernesystemene for KraftCERTs medlemmer. IT støtter driften, men det er effekten på kontrollsystemene og på leveransen som avgjør hvor alvorlig et cyberangrep er for våre sektorer.

Dette kapittelet strukturerer OT-trusselen etter effektkategori: ubetydelige angrep, disruptive angrep og destruktive angrep. Skillet er analytisk viktig fordi de tre kategoriene har ulik sannsynlighet, stiller ulike krav til angriperen og rammer ulike virksomheter ulikt.

OT-systemer har ulik sikkerhetsmodenhet avhengig av sektor og funksjon. De er underlagt regelverk og retningslinjer basert på kritikalitet, som legger føringer for sikkerhetstiltak, barrierer og infrastruktur.

4.1 Ubetydelige angrep / Nuisance attacks

En tydelig trend de siste årene er enkle angrep fra opportunistiske trusselaktører som Hacktivister og såkalte faketivister, som på bakgrunn av geopolitiske hendelser retter seg mot sårbare og tilgjengelige OT-systemer. Disse aktørene opererer systematisk ved å identifisere internetteksponerte enheter som PLC-er[6], HMI-er[7] eller andre OT-komponenter med manglende grunnsikring, og angriper disse. Angrepene mot israelske Unitronics-enheter høsten 2023, utført av Iran-tilknyttede hacktivister, illustrerer denne fremgangsmåten. Felles for alle berørte systemer er at de var direkte tilgjengelige fra Internett og manglet grunnleggende OT-sikring[8].

Det er nesten sikkert (> 90%) at russiske hacktivister vil fortsette å angripe sårbare, internetteksponerte OT-systemer. Disse aktørene har demonstrert interesse for å ramme OT-systemer både i Europa og i Norge. Systemer som mangler grunnsikring er særlig utsatt for hacktivisters enkle angrepsteknikker.

Det er lite sannsynlig (25–40%) at hacktivister oppnår driftsforstyrrende effekt ved angrep på enkle, internetteksponerte OT-systemer. De søker enkle og sårbare mål, og ved kompromittering manipuleres prosessfunksjoner opportunistisk. Aktørgruppene er aktive i sosiale medier, hvor de publiserer dokumentasjon fra kompromitterte systemer og fremmer påstander om angrep. Disse gruppene handler i stor grad på bakgrunn av geopolitiske hendelser og opererer i politiske gråsoner. OT-systemer som følger grunnsikring i henhold til regulering og retningslinjer er robuste mot denne typen aktører.

> ***Ubetydelige angrep: Angrepsmulighet følger sikringsgrad.***
>
> Virksomheter med grunnsikring på plass, typisk de som er underlagt effektivt sektorregelverk, vil oppleve dette som et støyproblem. For virksomheter uten tilsvarende sikringsgrad er det samme angrepet den mest sannsynlige og mest konkrete trusselen de står overfor.
>
> Dette er et valg på to nivåer: det valget virksomheten tar om egen sikring, og det valget myndighetene tar om hva som trenger regulering. Anlegg med betydning for kraftforsyningen eller petroleumsleveranser er regulert og derfor lite sårbare for denne type angrep.
>
> Utenfor regulering finnes mange mindre systemer med mangelfull sikring der et angrep primært får konsekvenser for eierne, fra vindparker til grusentreprenører.

[6] Programmable logic controller
[7] Human-machine interface
[8] https://claroty.com/resources/reports/analyzing-cps-attack-trends

4.2 Disruptive angrep og driftsforstyrrelser

Disruptive angrep har som mål å forstyrre virksomhetens leveranser. Dette kan gjøres ved angrep direkte mot kontrollsystemer, eller indirekte ved å angripe støttesystemer som er nødvendige for drift. Samtidig kan andre angrep utilsiktet forårsake samme effekt.

Det er sannsynlig (55–70%) at trusselaktører vil gjennomføre angrep med så store konsekvenser at det får driftsforstyrrende effekt. Det er virksomhetenes usikkerhet om angrepenes omfang som fører til preventive nedstengninger eller isolering. Driftsavhengige komponenter og prosesser innenfor OT-sonen kan bli tvunget til nedstenging som en konsekvens av et angrep i IT-sonen. Isolering er en viktig metode for å hindre spredning til sikre soner, mens nedstenging av prosesser er ofte et sikkerhetstiltak som er designet for å hindre uønskede fysiske konsekvenser. Begge gir angrepet en reell driftsforstyrrende effekt. Konsekvensene kan strekke seg fra kortvarige driftsavbrudd til langvarig produksjonsstans.

> ### *Jaguar Land Rover-angrepet (JLR)*
>
> **Et IT-angrep i august 2025 påførte Jaguar Land Rover en langvarig driftsstans[9].** Mediadekningen kunne gi inntrykk av at OT ble kompromittert i angrepet, men realiteten er at både OT og tilhørende produksjonssystemer og anlegg ble stengt ned for å minimere risiko. I tillegg ble mange underleverandører direkte berørt av stansen.
>
> Dette er et eksempel på at de store avhengighetene mellom IT og OT fører til en lengre disruptiv effekt. Flere av de påståtte OT-angrepene som beskrives i media og på sosiale medier er ikke angrep direkte mot OT-enheter eller -infrastruktur. Dette er en sammenblanding av effekt og sårbarhet som kan føre til at man fokuserer på å fikse feil problem.

Det er meget sannsynlig (75–85%) at løsepengeangrep mot IT-systemer gir indirekte effekter, inkludert driftsforstyrrelser. Slike angrep kan utløse forsvarstiltak som isolering eller nedstenging av OT og produksjon for å hindre videre eskalering. Det finnes mange funksjonelle avhengigheter mellom IT og OT som et løsepengeangrep kan ramme, og som kan tvinge virksomheten til å gjennomføre nedstenging som et risikoreduserende tiltak.

Det er meget lite sannsynlig (15–20%) at angripere vil lykkes med direkte tjenestenektangrep mot OT-utstyr. Slike enheter er gjemt bak flere lag sikringstiltak som segmentering og tilgangskontroll som må omgås, eller krever fysisk tilgang. Unntaket er usikret og sårbart utstyr koblet direkte til Internett.

Det er sannsynlig (55–70%) at nasjonalstatlige aktører vil utføre disruptive angrep mot virksomhetene ved en forhøyet sikkerhetspolitisk situasjon, slik som i opptakten til krig. Ved større sikkerhetspolitiske endringer kan trusselaktører være særlig interessert i å utnytte alle mulige former for avhengigheter mellom OT- og IT-systemer.

Driftsforstyrrelse: forårsaket av forsvaret, utløst av angrepet

Et cyberangrep trenger ikke å nå OT for å påvirke driften. Det holder at situasjonen er uavklart. Samtidig er ikke alle driftsforstyrrelser like alvorlige. KraftCERT deler inn i 3 nivåer:

- Frakobling: Å stenge kommunikasjon mellom OT- og IT-sonene er et forsvarstiltak, ikke et tegn på kompromittering. Anlegget fortsetter å levere, men uten støttesystemer og overvåking fra IT-siden.
- Øydrift: Mer inngripende. Produksjonsenhetene opererer uavhengig av hverandre, uten sentral koordinering.
- Nedstenging: Dette er det mest inngripende, enten som en aktiv beslutning av virksomheten, eller utløst automatisk av sikkerhetssystemer designet nettopp for dette: å stanse prosessen kontrollert før situasjonen eskalerer.

4.3 Destruktive angrep

Destruktive angrep har som formål å påføre fysisk skade på infrastruktur, utstyr, miljø eller mennesker, altså skade som ikke lar seg rette opp ved gjenoppretting av systemer.

Det er meget lite sannsynlig (15–20%) at vi ser vellykkede destruktive angrep gjennomført mot OT-systemer i løpet av det neste året. Destruktive og målrettede angrep mot OT-systemer er svært ressurskrevende og teknisk krevende å gjennomføre. Et slikt angrep forutsetter at trusselaktøren evner å manipulere et bredt sett sikkerhetsmekanismer og omgå flere lag av barrierer. Der produksjonsprosessen er koblet til safety-systemer, øker kompleksiteten ytterligere. Det kreves dyp innsikt i og detaljert kunnskap om det konkrete OT-systemet og dets tilknytning til de fysisk styrte prosessene for å omgå forriglinger.

Skadevare med destruktiv effekt i OT-systemer er svært ressurs- og tidkrevende å utvikle, teste og ikke minst bruke med tilstrekkelig presisjon mot et utvalgt mål. En slik operasjon krever detaljert planlegging og målkunnskap, involvering av ulike fagmiljøer, og tilpassede angrepsteknikker og verktøy for hvert enkelt mål siden hvert mål er unikt. Skadevaren som benyttes må tilpasses de sårbarheter og angrepsflater trusselaktøren velger å utnytte. Sårbarheter og angrepsflater endrer sin eksponering gjennom systemets levetid, etter hvert som svakheter lukkes og tiltak implementeres. Dette innsnevrer gradvis trusselaktørens muligheter.

5 Kunstig intelligens (KI) i trusselbildet

KI endrer tempoet i angrepsutviklingen, men foreløpig ikke de grunnleggende skillene i trusselbildet. Dette kapittelet behandler KI som en tverrgående faktor; konkrete utslag er omtalt under Aktører og Teknikker.

Det er meget sannsynlig (75–85%) at KI øker angrepsvolumet, særlig fra mindre avanserte aktørtyper. Skanning, phishing, skadevareproduksjon og tilpasning av innhold blir raskere og billigere. Ressurssvake grupper som hacktivister får skaleringsevne uten å få bedre teknisk kapabilitet. Effekten på kort sikt er kvantitativ, ikke kvalitativ. Det er svært vanskelig å predikere hvor mye volumet vil øke. Både hvor raskt angripere tar i bruk nye teknikker, og hvor raskt forsvarere får effekt av sine KI-verktøy, er usikkert.

Det er meget sannsynlig (75–85%) at KI utvider informasjonsinnhentingen mot KraftCERTs medlemmer. Både statlige aktører og kriminelle tilretteleggere bruker KI til dette. Systematisering og sammenstilling av åpen informasjon er en oppgave KI løser godt, og informasjon som tidligere krevde manuell innsats, blir nå tilgjengelig og håndterbar i et omfang som kan utvide angripernes målutvalg. Særlig gjelder det tilsynelatende uskyldig eller fragmentert informasjon som kan gi angriper innsikt når det settes sammen over tid.

Det er sannsynlig (55–70%) at KI-bruk vil bli en angrepsflate hos KraftCERTs medlemmer. Når virksomheter tar i bruk KI-verktøy og KI-agenter, oppstår det nye inngangsporter og nye muligheter for lateral bevegelse i et angrep. KI-tjenester som behandler e-post er sårbare for fordekte kommandoer, KI-agenter med utvidede rettigheter kan kompromitteres for å oppnå dypere fotfeste, og skygge-KI gir eksfiltrasjonsmuligheter utenfor virksomhetens kontroll. Her er KI både sårbarhet for forsvareren og verktøy for angriperen. Vurderingen er usikker, både intern og ekstern KI har kort fartstid og er lite prøvd mot reelle angrep.

Det er lite sannsynlig (25–40%) at angrep utføres av KI-agenter alene på kort sikt. Iverksettelsesfasen og enkelte terskler krever fortsatt menneskelig vurdering, særlig ved angrep mot godt sikrede mål. Kravene til målkunnskap, ressursbruk og tilgang som skiller støy fra alvorlige angrep står uendret. Vurderingen er usikker blant annet fordi de tersklene den bygger på i forsvaret også kan bli utfordret av virksomhetenes egen KI.

Det er mulig (45–50%) at samhandling mellom KI-agenter blir en egen angrepsvei på lang sikt. Når egne og leverandørers KI-agenter begynner å samhandle direkte, skapes tillitsforhold angriperen kan utnytte uten å måtte kompromittere agentene selv. Leverandørangrep kan da bli en form for LOTL[9] på samme måte som en ubevoktet fjernaksess i dag. Usikkerheten ligger først og fremst i om virksomheter klarer å ta i bruk teknologien med sikkerhet i bunnen.

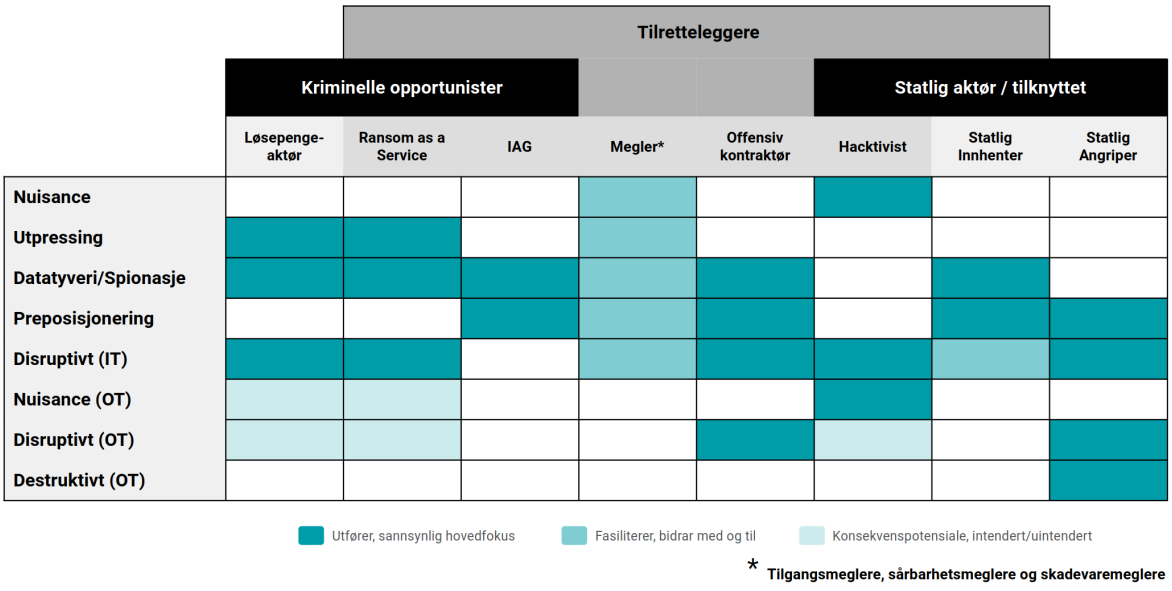
KI øker tempoet i kappløpet forsvarerne står i, og angripernes metoder blir raskere og enklere å utvikle. Virksomheter som digitaliserer uten kontroll på nye eksponeringer, utvider angripernes handlingsrom.

[9] Living off the Land

6 Aktører

6.1 Overordnet

Bak trusselbildet beskrevet i Situasjonsbildet, opererer aktører i et økosystem av tjenester, verktøy og samarbeid. Modellen viser hvordan ulike aktørtyper (tilretteleggere, kriminelle, hacktivister og statlige aktører) benytter eller kjøper tjenester som tilganger, skadevareutvikling, rekognosering og hjelp til eller utførelse av angrep. Modellen er ment å vise hvordan dette mørke eller grå markedet muliggjør angrep som spionasje, utpressing, preposisjonering og direkte skade. KraftCERT vurderer at de aller fleste trusselaktører, uavhengig av type og motivasjon, primært velger mål ut fra tilgjengelig mulighet.



Figur 1: Sammenheng mellom aktører, tjenester og angrepsformer

6.2 Tilretteleggere

Det finnes et stort marked med aktører som tilrettelegger for angripere. Disse utfører ikke selv angrep direkte på mål, men tjener penger på å legge til rette for slike angrep både for kriminelle og oppdragsstyrte aktører. Dette kan gjøres på mørke eller grå markeder.

6.2.1 Tjenesteleverandører

Både kriminelle og oppdragsstyrte aktører kjøper tilgang til mål via sårbarheter eller innloggingsdetaljer. Kjøp og salg av sårbarheter er en meget lukrativ aktivitet. Spesialiserte meglere som Zerodium[10] opererer i gråsonen mellom lovlig og ulovlig virksomhet – de kjøper ukjente sårbarheter fra sikkerhetsforskere og selger dem videre, typisk til etterretnings- og politimyndigheter. I det kriminelle segmentet omsettes også eldre eller allerede brukte sårbarheter på lukkede fora på det mørke nettet, tilgjengelig for aktører med langt lavere budsjetter enn nasjonalstater.

Det er sannsynlig (55-70%) at verktøy som brukes til spionasje mot nasjonalstater også brukes mot virksomheter i våre sektorer. Verktøy som infostealere finner veien fra statlige til kriminelle aktører og

[10] https://en.wikipedia.org/wiki/Zerodium

vice versa. Det finnes flere såkalte «gråsoneaktører»[11] som selger ferdige spionasjeverktøy til myndigheter og som brukes til overvåking av journalister og menneskerettighetsforkjempere ved å utnytte sårbarheter i personlige enheter som telefoner og datamaskiner.

KI brukes til å kartlegge (samle og sammenstille) informasjon om mål, og dette har gjort slike operasjoner betydelig enklere og raskere å gjennomføre. KraftCERT har tidligere skrevet om IAGer[fn:Initial Access Group]/meglere som samler og/eller selger initiell tilgang til virksomheter, og antallet slike grupper har økt. Vi vurderer at dette vil gjelde fremover både på kort og lengre sikt.

6.2.2 Offensive kontraktører

Det er meget sannsynlig (75–85%) at nasjonalstatlige aktører leier inn «hackers for hire» for å delta i eller utføre angrep alene[10] [11]. Dette kan være aktører på det mørke nettet eller legitime sikkerhetsselskaper i mange land, inkludert Kina, Russland, USA, eller Europa[12]. Spesielt i Kina er linjen mellom statlige og kommersielle aktører nesten visket ut, men både Russland og USA har utstrakt bruk av kontraktører i sikkerhetsarbeid, også offensivt[8].

6.2.3 Innsidere

Innsidere som bevisst tilrettelegger for angrep har et stort konsekvenspotensial for virksomheter, men det er en trussel med lav sannsynlighet.

Det er lite sannsynlig (25–40%) at en innsider vil bli presset til å utføre eller delta i disruptive eller destruktive angrep. En aktiv innsider i effektoperasjoner tar stor risiko, spesielt hvis angrepet har en fysisk komponent. Handlingene etterlater spor som kan fanges opp i logger og krever omgåelse av kontrolltiltak. Trusselaktøren brenner den ressursen en innsider er, så selv om risikoviljen til Russland er økende, må måloppnåelsen være stor for å rettferdiggjøre bruken.

Derimot er det sannsynlig (55–70%) at en trusselaktør vil forsøke å få innsidere til å skaffe informasjon som kan brukes i senere cyberoperasjoner. En etablert innsider som utsettes for press eller trusler er en reell kilde til informasjonslekkasje, og det er dette som gjør innsiderekruttering attraktivt for trusselaktører.

Trusselaktører benytter blant annet sosiale medier i forsøk på å rekruttere innsidere. Fremveksten av «crime-as-a-service» i det fysiske domenet viser at dette skjer, og at det kan foregå på en mer fordekt måte enn tradisjonell rekruttering.

[11] Lovlige selskaper som kjøper og selger til både legitime aktører og kriminelle

Innsidetrussel: lav, ukjent, men reell

Innsidetrusselen er reell med stort skadepotensial, men sannsynligheten for en gitt virksomhet er nærmest umulig å fastslå.

En gjennomgang fra FOI av europeiske spionasjesaker[13] mellom 2008 og 2024 identifiserte kun 70 saker, ingen fra Norge eller Island. KraftCERTs egen spørreundersøkelse blant medlemmer viser det samme mønsteret: 72% har ikke erfart innsiderhendelser, mens 77% har erfart utilsiktede feil med sikkerhetsmessige konsekvenser.

KraftCERTs forskningsrapport om utnytting av personell[14] fra 2025 peker på at feltet mangler felles begrepsapparat og gode indikatorer, noe som gjør presis vurdering vanskelig for alle, både sikkerhetsmyndigheter, KraftCERT og virksomhetene.

Det analytisk viktige skillet er mellom forsettlig innsidehandling og utilsiktede feil. Disse krever ulike vurderinger og ulike tiltak.

6.3 Cyberkriminelle

Kriminelle vil også fremover være den mest sannsynlige angriperen mot våre medlemmer. Kriminelle aktører er ute etter å tjene penger. De vil drive utpressing eller selge informasjonen de finner. De skanner konstant etter tekniske sårbarheter (se Direkte teknisk tilgang) og antallet aktører som er ute etter å tilegne seg tilganger gjennom phishing er økende (se Tjenesteleverandører).

Kriminelle aktører ser våre medlemmer som attraktive mål. Nesten alle våre medlemmer er små eller mellomstore selskaper, og aktørene ser dem som enklere å både utnytte og å til å ha betalingsvilje. Større selskaper har ofte både høyere sikringsgrad og policy om å ikke betale ut løsepenger [12]. At elkraft og petroleum sees på som en sektor i USA ("Energy"), med stor inntjening og betalingsvilje, gjør det rimelig å anta at en del enklere kriminelle grupper tror at det samme gjelder selskaper innen energisektorene i Norge.

Globalt ser antallet rapporterte løsepengeangrep ut til å fortsette å øke, mens utbetalingene er stabile eller synkende. Årsaken er forbedret sikkerhetsarbeid i vestlige land, og spesielt i Norden. Dette vil på sikt føre til avtakende avkastning for løsepengeaktører, og at de flytter seg til å angripe områder som er mindre modne sikkerhetsmessig.

Kriminelle aktører som ikke kan utnytte kompromitterte tilganger eller informasjon selv, selger eller bytter dem på ulike arenaer. Dette gjelder på tvers av aktørtyper og er en etablert del av den kriminelle økonomien.

Det er lite sannsynlig (25–40%) at myndighetsaksjoner har effekt på cyberkriminelle grupper på lang sikt. Myndigheter i både Europa og USA har gjennomført mange aksjoner i form av nedtakinger av kriminelle gruppers infrastruktur det siste året. Mange aktører starter likevel opp igjen etter at de har etablert ny infrastruktur for angrep. Det er også vanskelig å pågripe personer i grupper som har tilholdssted i land uten utleveringsavtale.

Det er et økende antall kriminelle grupper som utfører angrep. Årsaken er sannsynligvis fragmentering på grunn av myndighetsaksjonene, og at en større andel av kriminaliteten gjøres på nett.

[12] Tiltakspakke 2025 - Opprett rutine for løsepengeangrep (7413)

Det er meget sannsynlig (75–85%) at leverandører til sektorene våre vil bli angrepet av utpressingsaktører. Spesielt vil mindre selskaper som ikke er underlagt myndighetsregulering være utsatt, og ofte ha lavere bevissthet og kunnskap om IT-sikkerhet. Det er mindre sannsynlig at større leverandører blir angrepet, men angrep mot disse vil ha en mye større effekt på virksomhetene som bruker leverandøren. Avhengig av typen leveranse vil slike selskaper ofte ha flere og dypere direkte tilganger til virksomheten, noe som kan føre til større usikkerhet.

Det er meget sannsynlig (75–85%) at større leverandører vil holde tilbake informasjon om cyberangrep, eller kun dele det som er strengt nødvendig. Større selskaper har større omdømmerisiko ved angrep enn små selskaper, og vil forsøke å styre narrativet. KraftCERT har selv erfart dette under hendelser.

Det er meget sannsynlig (75–85%) at trusselaktører vil kompromittere mål via kode tilgjengelig på internett. Det har det siste året vært mange eksempler at GitHub-repoer og pakker som inkluderes i JavaScript-kode[13] eller Python-pakker[14] har blitt injisert med ondsinnet kode. Dette er en enkel måte for trusselaktører å få fotfeste på innsiden, enten hos virksomheten selv eller via en leverandør. Slike koderepoer har i noen tilfeller vært en kilde til at trusselaktører kan skaffe seg innloggingsdetaljer eller stjele informasjon.

6.4 Oppdragsstyrte aktører

Angrepskapasitet er viktigste ambisjon for statlige aktører på lang sikt. I den geopolitiske konkurransen ønsker stater å ha mulighet til å kunne ramme kritiske mål hos motstandere. Målstyrte eller oppdragsstyrte aktører har i hovedsak en annen motivasjon enn det rent økonomiske.

På kort sikt er likevel muligheten for å gjennomføre angrep viktigere for målutvelgelse enn å gå etter spesifikke virksomheter, slik angrepet på polske vindkraftverk i 2025 viser. Dårlig sikring av internetteksponert utstyr gir angripere mulighet til å ta seg inn i en sektor som vanligvis er vanskelig å kompromittere, og de velger å utnytte denne muligheten for å oppnå andre typer effekter enn de fysiske konsekvensene, for eksempel som ledd i en propagandakampanje for å skape usikkerhet.

6.4.1 Nasjonalstater

Russland vedlikeholder tvetydigheten mellom statlig, statsstøttet og prorussisk aktivitet som et strategisk virkemiddel. Det er nesten sikkert (> 90%) at Russland vil fortsette å støtte, veilede og utnytte hacktivister og prorussiske grupper til angrep mot norsk infrastruktur. KraftCERTs vurdering av disse aktørene er omtalt i kapittelet om Hacktivister.

Det er meget lite sannsynlig (15–20%) at Russland vil gjennomføre angrep med destruktiv effekt mot norske virksomheter. Vurderingen er uendret fra KraftCERTs analyser i både 2023, 2024 og 2025. Målrettede destruktive cyberangrep mot industrielle kontrollsystemer krever store ressurser over lang tid og har stort potensiale for konflikteskalering. Selv om Russland virker å ha høyere risikovilje har de fortsatt mye ressurser bundet opp i krigen mot Ukraina, og det vil derfor ta tid før de har bygget kapasitet til å gjennomføre vellykkede angrep mot infrastruktur av betydning.

KraftCERT mener det er lite sannsynlig (25–40%) at Russland vil gjennomføre cyberangrep som gir direkte disruptiv effekt/driftsforstyrrelser mot våre sektorer på kort sikt. Selv om angrepene mot Ukraina fortsetter, er det nå en dreiing mot mer spionasjeaktivitet og færre angrep med direkte effekt. Målet med slike angrep i Ukraina er nå å skremme vekk personell for å forsinke gjenoppretting, eller å innhente informasjon etter kinetiske angrep.

[13] https://en.wikipedia.org/wiki/Npm
[14] https://en.wikipedia.org/wiki/Python_(programming_language)

Alle nasjonalstater med offensive kapabiliteter vil forsøke å bygge evne til cyberangrep. Likevel har vi sett få angrep med stor effekt, også i konfliktsituasjoner. Når en konflikt oppstår vil stater bruke de midlene og mulighetene de har til rådighet, uavhengig av reelt effektpotensial. Et slikt eksempel er Irans angrep på medisinutstyrsprodusenten Stryker, som viser at statlige aktører også angriper virksomheter som bare perifert påvirker forsvarsevnen.

Nasjonalstatlige aktører bruker åpent tilgjengelig informasjon om virksomheter i våre sektorer til å finne sårbarheter og planlegge angrep. Bruk av KI av både egne (se kap. 7 Teknikker) og innleide ressurser (kap. 6 Tilretteleggere) gjør at omfanget av slik innsamling har potensial til å øke dramatisk. Økt evne til systematisering og sammentilling av slik åpen tilgjengelig informasjon kan gi flere muligheter til angrep.

Det er meget sannsynlig (75–85%) at kinesiske aktører vil hente inn informasjon fra våre sektorer. Innhentingen kan rette seg mot teknologisk innsikt og programvaresårbarheter som kan gi tilgang til norske virksomheter eller styrke kinesisk handlingsrom over tid[1][5]. Kinesiske aktører søker samtidig å skjule både metode og tilknytning[5]. Dette gjøres ved at de benytter seg av legitime skytjenester for å gjennomføre fordekte operasjoner.

Det er også sannsynlig (55–70%) at kinesiske aktører retter seg mot telekomindustri mot utstyr fra utvalgte virksomheter og leverandører, og ofte angriper nettverksutstyr (se Direkte teknisk tilgang) de kjenner til eller utstyr hvor de har god innsikt i sårbarhetene. Angrepene vil meget sannsynlig (75–85%) gjøres gjennom angrep direkte på virksomhetene eller via leverandør. PST beskriver Salt Typhoon[15] som et eksempel på at kinesiske aktører har kompromittert sårbare nettverksenheter hos en norsk virksomhet[5]. Denne aktiviteten er ikke observert i KraftCERTs sektorer.

Det er meget lite sannsynlig (15–20%) at Kina vil utføre disruptive eller destruktive angrep mot våre sektorer. Kravene til ressursbruk er de samme for Kina som for Russland, og Kina er ikke i direkte konflikt med Norge eller Europa. Likevel vurderer KraftCERT at det er mulig (45–50%) at de forsøker å preposisjonere seg for senere angrep.

Iran og Nord-Korea vurderes som mindre relevante trusselaktører for våre sektorer. Iran er løftet tydeligere i PSTs vurdering for 2026, men målbildet er særlig dissidenter, kritikere, israelske interesser og andre vestlige mål[5]. Iranske hacktivister kan i ytterste konsekvens angripe norske selskaper på grunn av en opplevd solidaritet mellom Norge og USA, men dette fremstår som lite sannsynlig (25–40%). Nord-Korea er oftere relevant gjennom kryptosvindel og forsøk på å få nordkoreanske IT-utviklere inn i vestlige virksomheter under falsk identitet[5]. Det er relevante trusler på samfunnsnivå, men mindre sentrale for våre sektorer enn russisk og kinesisk aktivitet.

6.4.2 Hacktivister

Politisk baserte hacktivister forsøker å utføre angrep mot sine motstandere, eller forsøker å koble mer tilfeldige mål til sin politiske sak. Hacktivismebegrepet omfatter både nasjonalstatlige, statsstøttede, statsvennlige og ideologisk drevne aktører.

Hacktivister er løst organiserte grupper av personer med en uttalt intensjon om å gjøre angrep med en politisk agenda for en stat eller statsliknende opprørsgruppe. De kan være støttet av nasjonalstater, men dette er ikke nødvendig. Det finnes også «faketivister»: statlige aktører som gir seg ut for å være hacktivister for å kunne unngå attribusjon.

I motsetning til den klassiske definisjonen av hacktivist som en rent ideologisk aktør, velger hacktivister i dag mål basert på pågående politiske og regionale konflikter. Målet med angrepene er propaganda og å

[15] https://en.wikipedia.org/wiki/Salt_Typhoon

skape uro i landene som angripes. Ofte ser man en dreiing av målutvelgelse ut fra geopolitiske hendelser slik vi har sett etter angrepene mot Ukraina, Gaza og Iran.

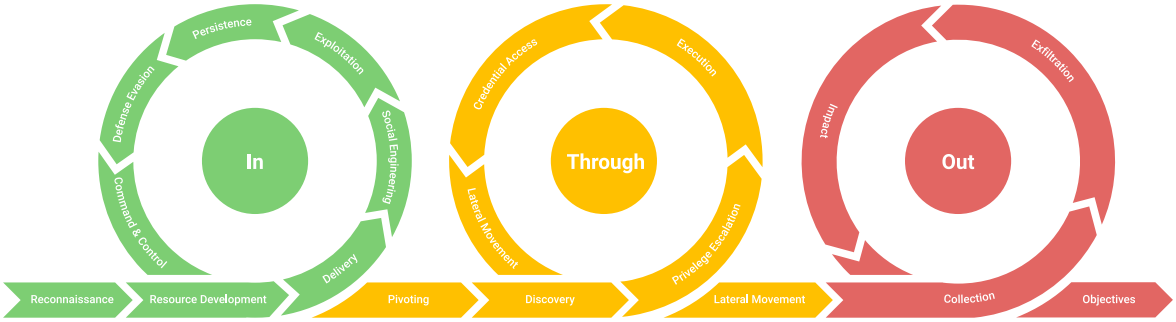
Det er meget lite sannsynlig (15–20%) at innenlandske aktivister vil forsøke å gjennomføre cyberangrep mot våre sektorer, som f.eks. lokale vindkraftmotstandere eller klimaaktivister.

Det er meget sannsynlig (75–85%) at russisk-støttede aktører vil utføre angrep mot dårlig sikret infrastruktur i Norge det neste året. Det er sannsynlig (55–70%) at pro-russiske hacktivister vil angripe svakt sikrede OT-systemer, men det er lite sannsynlig (25–40%) at de klarer å gjennomføre angrep på OT-systemer som er innenfor godt sikkerhetsregulerte sektorer eller virksomheter som har grunnsikring på plass.

Det er meget sannsynlig (75–85%) at statlig støttede hacktivister får hjelp fra statlige aktører til både målutvelgelse og tilgang til verktøy. Åpne tilganger, enten via sårbarheter eller tilgangsdetaljer, er hovedgrunn til målutvelgelse for hacktivister. KI gjør at selv ressurssvake hacktivistgrupper kan skanne og kartlegge flere mål enn tidligere, uten at de dermed har fått bedre teknisk evne til å gjennomføre mer avanserte angrep.

7 Teknikker

7.1 Unified Kill Chain



Figur 2: Unified Kill Chain (UKC)

Trusselaktører bruker mange av de samme teknikkene, uavhengig av hvem de er og hva de vil. Dette kapittelet beskriver angrepskjeden strukturert etter Unified Kill Chain: tilgang, bevegelse og iverksettelse. Tilgangsfasen handler om å komme inn, bevegelsesfasen om å spre seg videre uten å bli oppdaget, og iverksettelsesfasen om å gjennomføre det angriperen kom for.

7.2 Tilgang (In)

7.2.1 Kartlegging og målutvelgelse

KraftCERT vurderer det som nesten sikkert (> 90%) at oppdragsstyrte aktører vil skanne alle våre medlemmers infrastruktur for å kartlegge enheter, nettverk og systemdetaljer. Skanningen gjøres som forberedelse til angrep, og gjøres av de fleste typer trusselaktører. Formålet er å finne potensielle mål hvor det er lite ressurskrevende å kompromittere, enten for enkle formål som propaganda eller for langsiktig preposisjonering.

Slik skanning utføres automatisert og i stor skala, i økende grad med KI-støtte, og gjør det mulig å identifisere angrepsflater i eksponerte tjenester, åpne porter og tekniske sårbarheter uten å direkte angripe målet.

For mer avanserte trusselaktører er kartlegging tett koblet til utnyttelse av kjente og ukjente sårbarheter, men også relativt enkle aktører skanner etter eksponert utstyr som har standardpassord.

7.2.2 Direkte teknisk tilgang

Eksponerte tjenester vil sannsynligvis være den viktigste inngangsporten. Fjerntilkoblingstjenester, som VPN eller spesiallagde tjenester, og -applikasjoner som VNC[16] dukker opp ved skanning da de er eksponert mot internett. Både legitime tjenester som Shodan[17], og trusselaktører skanner aktivt alle eksponerte internett-tjenester kontinuerlig.

Det er meget sannsynlig (75-85%) at trusselaktører vil forsøke å kompromittere (I)IoT-enheter som er eksponert på internett, da de har mange sårbarheter og er ofte usikret. IoT[18]-enheter settes ofte

16 Virtual Network Computing
17 https://www.shodan.io/
18 Internet of Things

opp uten aktiv bruk av virksomhetenes sikkerhetspolicy, eller av leverandører av spesialtjenester. Selv om disse ikke er direkte tilkoblet virksomhetens nettverk, vil angripere kunne bruke enhetene som springbrett eller til å samle informasjon.

Det er sannsynlig (55–70%) at sårbarheter i perimeterutstyr blir utnyttet av alle typer trusselaktører. Andelen vellykkede kompromitteringer som utnytter sårbarheter har økt, og gjøres av oppdragsstyrte aktører, kriminelle og tilretteleggere. Aktørene utnytter både kjente og ukjente sårbarheter, og såkalte «bruteforcing»[19]-teknikker.

Google Threat Intelligence Group registrerte i 2023-25 rett under 100 aktivt utnyttede zero-days, der over 40 prosent av disse rammet eksponert nettverksutstyr som VPN-er, brannmurer og rutere. Markedet for slike sårbarheter speiles direkte i angrepsmønstrene mot perimeterutstyr KraftCERT er kjent med i våre sektorer[15].

Det er meget sannsynlig (75–85%) at trusselaktører vil angripe gjennom skytjenester. Spesielt gjelder dette web- og skytjenester hvor legitime brukere benytter nettleser for funksjonen. Teknikker som ClickFix[16] kombinert med infostealere gir angripere mulighet til å stjele innloggingsdetaljer og -tokens for å kunne angripe eksponerte tjenester.



Figur 3: UKC - «In»

KraftCERT vurderer det som meget sannsynlig (75–85%) at kinesiske nasjonalstatlige aktører vil angripe utstyr fra spesifikke leverandører til telekomindustrien ved å utnytte sårbarheter de er kjent med. Oppdragsstyrte aktører har gjerne egen ekspertise og kunnskap om sårbarheter som ikke er offentlig kjent. Kinesiske myndigheter har også innført lovgivning hvor de har førsterett på alle sårbarheter som oppdages for å kunne ha disse i sine verktøykasser[17][18].

Det er sannsynlig (55–70%) at KI brukes til å utvikle angrepsskadevare til phishing- og deepfake-kampanjer. Angripere utnytter at autentisering av brukerkontoer uten phishing-resistent MFA[20] ofte er enkelt å omgå med phishing eller bruteforcing. Løsepengegrupper har i høy grad automatisert slike innbruddsprosesser. Dette har både redusert tiden en slik kompromittering tar og økt antallet angrep det er mulig å utføre.

Det er meget sannsynlig (75–85%) at KI-assistert skadevare på kort sikt vil redusere tiden en inntrenging tar i betydelig grad, og spesielt gjelder dette «Skadevare som tjeneste»(MaaS[21]). Utviklingen av KI-verktøy gjør at produksjonstiden for skadevare er redusert, og spesielt der hvor de er laget for å utnytte nylig kjente sårbarheter hentet fra varsler.

Det er meget sannsynlig (75–85%) at angripere på kort sikt vil forsøke å utnytte virksomhetenes egne KI-verktøy som inngangsport. Flere har tatt i bruk Copilot som verktøy for behandling av inngående e-post, og disse er sårbare for fordekte kommandoer usynlige for det menneskelige øye som behandles av KI-tjenesten[19].

Trusselaktører vil forsøke å kompromittere fjernaksess for å få tilgang til OT-systemer. Stjålet tilgangsinformasjon eller bruk av brute-force teknikker vil kunne knekke svakt sikrede autentiseringsmekanismer. Både eget personell og leverandører gjennom tjenesteutsetting har tilgang via slike løsninger, og brukerkontoer er av særlig interesse for trusselaktører.

19 Passordgjetting i stor skala
20 Multi-Factor Authentication
21 Malware-as-a-Service

Det er meget sannsynlig (75–85%) at angripere vil utnytte sårbare perimeterenheter som inngangsvektor til OT-sonene. Målrettede oppdragsstyrte trusselaktører skanner spesifikt etter sårbarheter spesielt i utstyr som finnes i perimeter til OT-sonen, som VPN-konsentratorer, brannmurer og andre tjenester som er tilgjengelig fra internett eller IT-sonen. Aktørene har et vindu mellom tidspunktet sårbarheter publiseres og utstyret patches som kan utnyttes, og som nevnt er tiden som trengs for skadevareproduksjon på vei ned.

7.2.3 Angrep gjennom leverandører

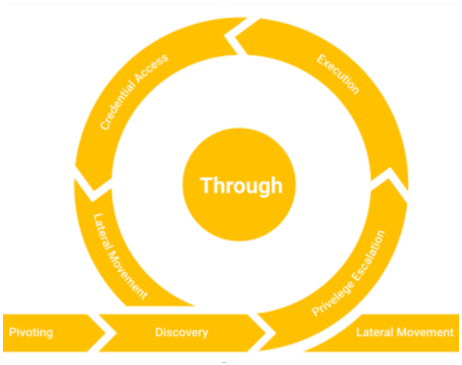
KraftCERT mener det er sannsynlig (55–70%) at angrepsforsøk vil skje gjennom kompromittering og utnyttelse av leverandører. Deres tillitsforhold til virksomhetene utnyttes til kompromittering via phishing. Merk at slike angrep vil kunne ha uintenderte effekter hos virksomhetene som fører til driftsforstyrrelser pga. usikkerhet, og føre-var-prinsippet.

KraftCERT mener det er meget sannsynlig (75–85%) at virksomheter i våre sektorer vil berøres av trusselaktørers angrep på kodelagre [20][21]. Utviklermiljøer benytter både åpne kodelagre som GitHub, eller trekker inn moduler eller biblioteker fra internett når de programmerer. Dersom en angriper inkluderer ondsinnet kode i egenutviklet kode gir dette muligheter for angrep direkte.

Opportunistiske aktører som angriper leverandører er på utkikk etter kontodetaljer til brukere som har utvidede rettigheter, spesielt til kunders systemer og infrastruktur. Fjernaksess er nevnt over, men også tilgang til kundenes data eller informasjon er meget interessant å få tak i. Slike data er høyst interessante, fordi tilganger enkelt kan selges. Informasjon om mål vurdert som kritisk infrastruktur kan også ha verdi i samspillet mellom kriminelle og russiske sikkerhetstjenester, der juridisk dekke for kriminell aktivitet rettet utenlands kan utveksles mot tjenester eller betaling[22].

7.3 Bevegelse (Through)

LotL[22] **er trusselaktørers foretrukne angrepsmetode.** De fleste angripere gjør sitt ytterste for å gli ubemerket gjennom sikkerhetssystemer og grensesnitt uten å bli oppdaget. Legitime verktøy vil også ha tilganger på tvers av soner som gir mulighet både for lateral bevegelse mellom endepunkter og bevegelse over grensesnitt som brannmurer.



Figur 4: UKC - «Through»

Angripere bruker legitime internettverktøy til kommando og kontroll. Disse har tilganger ut mot internett, og kan ikke enkelt blokkeres av virksomhetene uten at det får følger for normal internettbruk.

Det er sannsynlig (55–70%) at avanserte aktører vil forsøke å kompromittere KI-agenter som er i bruk hos virksomhetene for å oppnå dypere fotfeste i virksomhetens infrastruktur. Som eksempel kan en kompromittering av KI-agenter til utvikling av intern kode gi en angriper både innsikt og en enkel måte å rulle ut skadevare.

Det er sannsynlig (55–70%) at trusselaktører vil forsøke å angripe KI-tjenester for å samle informasjon før eksfiltrasjon[23]. Spesielt gjelder dette dette hvor virksomhetenes ansatte har tatt i bruk «skygge-KI»[23].

Det er nesten sikkert (> 90%) at trusselaktører utvikler og bruker skadevare spesifikt rettet mot alle typer operativsystemer. I tillegg utvikles skadevare mot hypervisere som VMware og Hyper-V, og kontainerteknologi som Kubernetes, Docker og liknende.

Det er sannsynlig (55–70%) at angripere vil utnytte manglende autentisering av trafikk til lateral bevegelse, både internt i prosessen mellom SCADA[24] og feltenheter og i integrasjoner som brukes til å utveksle data mellom OT- og IT-systemer. KraftCERT anser det som mulig (45–50%) at integrasjoner over internett angripes direkte, men vi har ikke sett bruk av slik teknikk ennå.

Det er meget sannsynlig (75–85%) at bruken av eldre protokoller utgjør en angrepsflate som trusselaktør kan utnytte, hvis de allerede har kommet seg på innsiden av perimeter til OT-sonen. Flere kommunikasjonsprotokoller har lav grad av sikkerhet siden det ikke var en del av det opprinnelige designet, slik som Modbus, Profibus og Elcom. Avanserte statlige aktører som Sandworm har vist at de har, og fortsetter å utvikle, kapabilitet til å utvikle angrepsteknikker mot ulik OT-teknologi for å kompromittere OT-systemer[24, s.1].

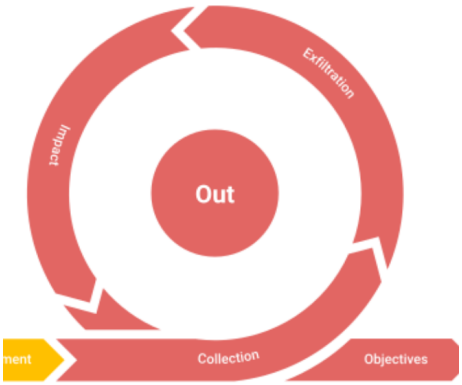
Det er meget sannsynlig (75–85%) at russiske statlige aktører har kapabilitet for å utnytte sårbare OT-systemer og kommunikasjonsprotokoller. Eldre systemer er ofte ikke mulig å oppdatere, har ikke samme sikkerhetsfunksjonalitet, og har mange sårbarheter i programvare og arkitektur som trusselaktør vil utnytte til fotfeste, bevegelse og effekt. Dersom det ikke er nok barrierer og robusthet i systemene, kan dette utnyttes av angriper dersom virksomheten ikke har god nok grunnsikring.

Det er sannsynlig (55–70%) at sårbarheter i virtuelle miljøer vil bli utnyttet av skadevare de neste årene. Virtualisering av OT-infrastruktur og bruk av virtuelle enheter og miljøer har økt betraktelig de siste årene - også i OT. Det er sannsynlig (55–70%) at OT-systemer, eller systemer med kobling til kontrollsystemet, som er plassert i sky vil angripes på samme måte.

22 Å leve av lendet, eng. Living off the Land
23 KI-bruk utenfor kontroll og policy
24 Supervisory Control and Data Acquisition

7.4 Iverksettelse (Out)

Angripere bruker legitime internettverktøy til å eksfiltrere data. Dette er ikke nytt, men økningen i antallet verktøy for fildeling og kommunikasjon gjør det vanskelig for virksomhetene å kontrollere bruken. Dette gjelder både angriperes og ansattes ilegitime bruk.



Figur 5: UKC - «Out»

På kort sikt er det lite sannsynlig (25–40%) at trusselaktører vil gjennomføre vellykkede angrep som er utført av KI-agenter alene. Det er derimot mulig (45–50%) at deler av iverksettelsesfasen utføres av KI-agenter med menneskelig oppfølging. Som nevnt har utpressingsaktørene allerede høy grad av automatisering, og med KI-støtte blir denne automatiseringen spredt til flere deler av angrepskjeden. Det er meget sannsynlig (75–85%) at KI brukes direkte i skadevareproduksjon.

Det er meget lite sannsynlig (15–20%) at vi vil se ransomware utviklet direkte mot OT-utstyr eller -systemer i løpet av det neste året. Slike systemer er annerledes enn vanlige IT-systemer, og det er derfor krevende å utvikle og få effekt på de delene av systemene som er OT-spesifikke. Det er enklere å bruke løsepengeskadevare mot IT-delene av slike systemer: operativ- eller filsystemet. Det siste kjente eksemplet på ransomware målrettet OT er EKANS[25] fra 2020.

Angripere har en stor verktøykasse med wipere. Slike verktøy kan ramme nær sagt alle typer utstyr. Wipere brukes for å slette data, konfigurasjon, operativsystem og firmware, og har vært mye brukt i Ukraina. Også skadevaren brukt i hendelsen i Polen har likhetstrekk med skadevare brukt av russiske nasjonalstatlige aktører.

Det er sannsynlig (55–70%) at OPC-UA som kommunikasjonsteknologi vil bli brukt i fremtidig skadevare mot kontrollsystemer. Bruk av OPC-UA[26] til kommunikasjon for datautveksling på tvers av soner i OT-systemet er en teknologiutvikling som følger av digitalisering og utvikling av «Industri 4.0»[27]. Flere OT-systemer og sektorer vil ta inn denne teknologien, noe som vil kunne medføre en økt mengde av homogene løsninger. Dette vil kunne gi trusselaktør økt mulighet for lateral bevegelse og tilgang til flere enheter og nettverk der OPC-UA brukes og hvor autentisering og verifisering av trafikk er mangelfull.

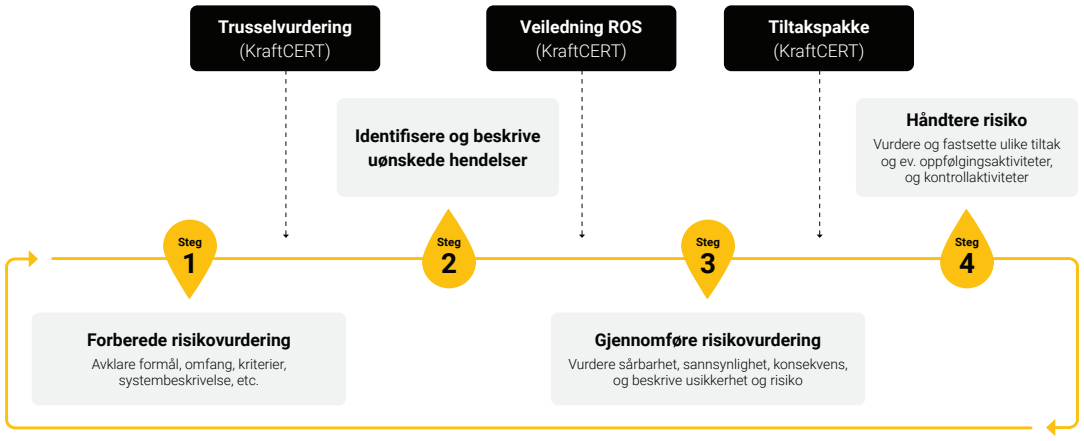
[25] https://malpedia.caad.fkie.fraunhofer.de/details/win.snake
[26] OPC Unified Architecture
[27] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

8 Om rapporten

8.1 Trusselvurdering og tiltakspakke

Trusselvurderingen følges opp med en tiltakspakke for medlemmer sommeren 2026. Den vil gi praktiske anbefalinger og forsøker å besvare hvordan truslene best kan møtes. Sammen kan disse bidra til virksomhetens ROS. Sikkerhet er billigst når det planlegges inn fra starten. Ny teknologi og nye integrasjoner øker angrepsflaten. Tiltakspakken gir konkrete anbefalinger, men det viktigste rådet kan gis allerede nå:

Sikkerhet må være et eget moment i all planlegging og utvikling, ikke noe som legges til i etterkant.



8.2 Trafikklysprotokollen

KraftCERT/InfraCERT bruker trafikklysprotokollen (TLP versjon 2.0) ved deling av informasjon for å angi hvordan informasjonen kan eller ikke kan deles videre.

Dette dokumentet er klassifisert som TLP:CLEAR. Informasjonen kan distribueres uten begrensninger.

Les mer om trafikklysprotokollen hos FIRST[28].

TLP:**RED**
Informasjon kun til individuelle personlige mottakere, ingen ytterligere formidling tillatt.

TLP:**AMBER** / TLP:**AMBER+STRICT**
Informasjon begrenset til tjenstlig behov i mottakers organisasjon og dens klienter. Kun i egen organisasjon hvis **STRICT**.

TLP:**GREEN**
Informasjonen kan formidles, men ikke publiseres.

TLP:**CLEAR**
Informasjon kan formidles uten begrensninger.

TLP v2.0

8.3 Endringslogg

Dato	Versjon	Beskrivelse
2026-04-30	1.0.0	Første utgivelse

[28] https://www.first.org/tlp

Referanser

[1] Etterretningstjenesten. *Fokus 2026*. 2. mar. 2026. URL: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20NO%20-%20Weboppslag%20v4.pdf.

[2] Forsvarets forskningsinstitutt. *Forsvarsanalysen 2025*. 17. feb. 2025. URL: https://www.ffi.no/publikasjoner/forsvarsanalysen-2025.

[3] Politiet. *Cyberkriminalitet 2026*. 17. mar. 2026. URL: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2026.pdf.

[4] Europol. *Steal, deal and repeat - Internet Organised Crime Threat Report 2025*. 13. jun. 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[5] Politiet. *Nasjonal trusselvurdering 2026*. 2. mar. 2026. URL: https://www.pst.no/wp-content/uploads/2026/02/Nasjonal-trusselvurdering-2026.pdf.

[6] EPRS. *Cloud and AI development act*. 1. apr. 2026. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779251/EPRS_BRI(2025)779251_EN.pdf.

[7] The White House. *IMPOSING SANCTIONS ON THE INTERNATIONAL CRIMINAL COURT*. 6. feb. 2026. URL: https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.

[8] The White House. *President Trump's CYBER STRATEGY for America*. 2. mar. 2026. URL: https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[9] CYFIRMA. *Investigation Report on Jaguar Land Rover Cyberattack*. 24. sep. 2025. URL: https://www.cyfirma.com/research/investigation-report-on-jaguar-land-rover-cyberattack/.

[10] Chatham House – International Affairs Think Tank. *Holding state-sponsored hackers and other cyber proxies to account*. 20. apr. 2026. URL: https://www.chathamhouse.org/2026/03/holding-state-sponsored-hackers-and-other-cyber-proxies-account.

[11] DeepStrike. *State-Sponsored Hacking: Global Trends and How to Defend in 2025*. 16. des. 2025. URL: https://deepstrike.io/blog/state-sponsored-hacking-apt-threats-2025.

[12] SpyCloud. *State Secrets for Sale: More Leaks from the Chinese Hack-for-Hire Industry*. 1. jul. 2025. URL: https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/.

[13] FOI Totalförsvarets forskningsinstitut. *"Spies Among Us": Espionage in Europe - A study on convicted spies in Europe 2008–2024*. 3. feb. 2026. URL: https://www.foi.se/rest-api/report/FOI-R--5866--SE.

[14] KraftCERT. *Forhindre utnytting av personell - Prinsipper og tiltak*. 13. nov. 2025. URL: https://www.kraftcert.no/filer/KraftCERT-utnytting-personell.pdf.

[15] Google Cloud. *Look What You Made Us Patch: 2025 Zero-Days in Review*. 5. mar. 2026. URL: https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review.

[16] Microsoft Security. *Think before you Click(Fix): Analyzing the ClickFix social engineering technique*. 21. aug. 2025. URL: https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/.

[17] Strategist. *China's vulnerability disclosure regulations put state security first*. 31. aug. 2021. URL: https://www.aspistrategist.org.au/chinas-vulnerability-disclosure-regulations-put-state-security-first.

[18] Atlantic Council. *Sleight of hand: How China weaponizes software vulnerabilities*. 13. mar. 2025. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability.

[19] CovertSwarm. *EchoLeak: The Zero-Click Microsoft Copilot Exploit That Changed AI Security*. 7. jul. 2025. URL: https://www.covertswarm.com/post/echoleak-copilot-exploit.

[20] The Register. *Two different attackers poisoned popular open source tools - and showed us the future of supply chain compromise*. 10. apr. 2026. URL: https://www.theregister.com/2026/04/11/trivy_axios_supply_chain_attacks.

[21] Datadog Security Labs. *Learnings from recent npm supply chain compromises*. 30. okt. 2025. URL: https://securitylabs.datadoghq.com/articles/learnings-from-recent-npm-compromises.

[22] Atlantic Council. *Unpacking Russia's cyber nesting doll*. 20. mai 2026. URL: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/.

[23] CSO Online. *Top 5 real-world AI security threats revealed in 2025*. 29. des. 2025. URL: https://www.csoonline.com/article/4111384/top-5-real-world-ai-security-threats-revealed-in-2025.html.

[24] CERT Polen. *CERT Polska Energy Sector Incident Report 2025*. 30. jan. 2026. URL: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.